AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

META PLATFORMS, INC. PROFILE ID ://www.facebook.com/profile.php?id=100087761752755

Case No. 3:23sw71

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 751(a)	Escape from Custody

The application is based on these facts:

See Attached Affidavit, including Attachments A & B

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

Michael C. Moore, Assistant U.S. Attorney
Printed name and title

Applicant's signature

Danielle Shimchick, Deputy U.S. Marshal
Printed name and title

Sworn to before me and signed in my presence.

Date: 05/04/2023

/s/ MRC
Mark R. Colombell
United States Magistrate Judge
Judge's signature

City and state: Richmond, VA

Mark R. Colombell, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF META PLATFORMS, INC. PROFILE ID ://www.facebook.com/profile.php?id=100087761752755	Case No. 3:23sw71 **FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT FOR STORED ELECTRONIC COMMUNICATIONS

I, Danielle Shimchick, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for Information associated with Meta Platforms User ID https://www.facebook.com/profile.php?id=100087761752755 (the "SUBJECT ACCOUNT") that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. ("Meta Platforms" or "the Provider"), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta Platforms to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the user ID. The items to be seized are described in the following paragraphs and in Attachment B.

2. I am a Deputy United States Marshal with the United States Marshals Service and have been since November 2009. During my tenure with the U.S. Marshals Service, one of

my primary duties has been the investigation of the whereabouts of federal and local fugitives. Based on my training and experience, fugitives routinely use Meta Platforms and social media accounts even while on fugitive status. Fugitives will typically communicate with friends via posts or Meta Platforms Messenger and disclose personal information regarding their whereabouts. Fugitives will often change the privacy settings to more restrictive means, to prevent law enforcement or other members of the public accessing their page. Throughout my career, I have learned access to Meta Platforms must be granted through an internet service provider (ISP) connection. Access to an ISP can be obtained through various means such as telephone lines, fiber optics, television cable and wireless Ethernet (wi-fi). Home ISP is generally obtained and paid for by family/friends, and fugitives often have access to the ISP. Typically, the ISP has location data, which would assist in determining a precise location for a fugitive.

3. Additionally, access to Meta Platforms through wi-fi will show the general location of a fugitive. As part of the USMS efforts to locate and arrest Bruce Carroll Callahan ("Callahan"), investigators need to obtain identifying information from the fugitive's Meta Platforms page and communications sent to or from the account associated with the subscriber. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts, as set forth in this affidavit, show that there is probable cause to search the information described in Attachment A for evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. § 751(a), Escape from the Custody of the U.S.

Attorney General, committed, and that are being committed, by Bruce Carroll Callahan. This evidence is further described in Attachment B.

RELEVANT STATUTORY PROVISIONS

4. On September 28, 2021, an arrest warrant and criminal complaint were issued in the Eastern District of North Carolina charging Bruce Carroll Callahan with Possession with Intent to Distribute Four Hundred (400) Grams or More of Fentanyl, in violation of 21 U.S.C. 841(a)(1) and related offenses. On November 23, 2021, an indictment was returned in that district under docket number 7:21-cr-138 charging Callahan with the following:

a. Count One - Conspiracy to knowingly and intentionally distribute and possess with intent to distribute a mixture and substance containing a detectable amount of fentanyl, cocaine and cocaine based, Schedule II controlled substances, in violation of Title 21, United States Code Section 846;

b. Count Two – Knowingly and intentionally distribute a quantity of cocaine of cocaine base (crack), in violation of Title 21, United States Code Section 841(a)(1);

c. Count Three - Knowingly and intentionally distribute twenty-eight grams or more of cocaine base (crack), a Schedule II controlled substance, in violation of Title 21, United States Code, Section 841(a)(1);

d. Count Four- Knowingly possess a firearm in furtherance of a drug trafficking crime for which he may be prosecuted in a court of the United States, in violation of Title 18, United States Code, Section 924(c) (1)(A);

e. Court Five – Knowingly and intentionally possessing with intent to distribute four hundred grams or more of a mixture containing fentanyl, a Schedule II controlled substance, in violation of Title 21, United States Code, Section 841(a)(1) and Title 18, United States Code, Section 2;

f. Count Six – Knowingly and intentionally possessing with intent to distribute a quantity of cocaine and quantity of cocaine base (crack), Schedule II controlled substances in violation of Title 21, United States Code, Section 841(a)(1); and

g. Count Seven – Knowingly possessing a firearm in furtherance of a drug trafficking crime for which he may be prosecuted in a court of the United States, in violation of Title 18, United States Section 924(c) (1)(A).

5. On August 17, 2022, Callahan appeared before Eastern District of North Carolina United States Magistrate Judge Robert B. Jones. Callahan was remanded to the custody of the Attorney General (via the United States Marshals Service) and placed in Robeson County Jail, 122 Legend Rd, Lumberton, NC 28358. Callahan was transferred from Robeson County Jail to Piedmont Regional Jail, 801 Industrial Park Rd., Farmville, VA 23901 on September 7, 2022 until his escape on April 30, 2023. Piedmont Regional Jail has a contract with the United States Marshals Service to house federal prisoners detained pending trial. Callahan was incarcerated at Piedmont Regional Jail pursuant to the detention order referenced above.

6. On May 1, 2023, the United States Marshals Service received notification from Piedmont Regional Jail regarding the escape of two federal inmates, Bruce Callahan and Alder Martin-Sotelo. On April 30, 2023, at approximately 2315 hours, Callahan escaped from

Piedmont Regional Jail, housing unit I-2. Callahan exited the facility through an unsecure door and scaled a fence by placing his t-shirt over the barbed wire. Callahan was last observed wearing only blue jail shorts. The shirt was later recovered containing blood. Piedmont Regional Jail is located within the Eastern District of Virginia.

7. A confidential source ("CS-1") stated that Callahan paid five thousand dollars for transportation arrangements regarding his escape. One thousand dollars was arranged for the driver of the vehicle scheduled to pick Callahan up, one thousand dollars for the subject supplying the vehicle, and three thousand dollars for the subject facilitating the transport.

8. Another confidential source ("CS-2") stated that the driver arrived at Piedmont Regional Jail on May 1, 2023, at approximately 0020 hours and waited until 0127 hours for Callahan. The driver departed without Callahan.

9. It is believed Callahan remains in, or around the Farmville area; however, his current whereabouts are unknown.

BACKGROUND CONCERNING META PLATFORMS

10. Meta Platforms owns and operates a free-access social networking website of the same name that can be accessed at http://www.Meta.com. Meta Platforms allows its users to establish accounts with Meta Platforms and users can then use their accounts to share written news, photographs, videos, and other information with other Meta Platforms users, and sometimes with the general public.

11. Meta Platforms asks users to provide basic contact and personal identifying information to Meta Platforms either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Meta

Platforms passwords, Meta Platforms security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Meta Platforms also assigns a user identification number to each account.

12. Meta Platforms users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Meta Platforms assigns a group identification number to each group. A Meta Platforms user can also connect directly with individual Meta Platforms users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Meta Platforms and can exchange communications or view information about each other. Each Meta Platforms user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

13. Meta Platforms users can select different levels of privacy for the communications and information associated with their Meta Platforms accounts. By adjusting these privacy settings, a Meta Platforms user can make information available only to himself or herself, to particular Meta Platforms users, or to anyone with access to the Internet, including people who are not Meta Platforms users. A Meta Platforms user can also create "lists" of Meta Platforms friends to facilitate the application of these privacy settings. Meta Platforms accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Meta Platforms.

14. Meta Platforms users can create profiles that include photographs, lists of personal interests, and other information. Meta Platforms users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Meta Platforms users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Meta Platforms users can "check in" to particular locations or add their geographic locations to their Meta Platforms posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

15. Meta Platforms allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (*i.e.*, label) other Meta Platforms users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Meta Platforms's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

16. Meta Platforms users can exchange private messages on Meta Platforms with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Meta Platforms, which also stores copies of messages sent by the recipient, as well as other information. Meta Platforms users can also post comments on the Meta Platforms profiles of other users or on their own profiles; such comments are typically associated with a specific

posting or item on the profile. In addition, Meta Platforms has a Chat feature that allows users to send and receive instant messages through Meta Platforms. These chat communications are stored in the chat history for the account. Meta Platforms also has a Video Calling feature, and although Meta Platforms does not record the calls themselves, it does keep records of the date of each call.

17. If a Meta Platforms user does not want to interact with another user on Meta Platforms, the first user can "block" the second user from seeing his or her account.

18. Meta Platforms has a "like" feature that allows users to give positive feedback or connect to particular pages. Meta Platforms users can "like" Meta Platforms posts or updates, as well as webpages or content on third-party (*i.e.*, non-Meta Platforms) websites. Meta Platforms users can also become "fans" of particular Meta Platforms pages.

19. Meta Platforms has a search function that enables its users to search Meta Platforms for keywords, usernames, or pages, among other things.

20. Each Meta Platforms account has an activity log, which is a list of the user's posts and other Meta Platforms activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Meta Platforms page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Meta Platforms page. Meta Platforms Notes is a blogging feature available to Meta Platforms users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

21. The Meta Platforms Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Meta Platforms users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.

22. Meta Platforms also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

23. In addition to the applications described above, Meta Platforms also provides its users with access to thousands of other applications ("apps") on the Meta Platforms platform. When a Meta Platforms user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

24. Meta Platforms uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Meta Platforms user identification numbers; groups and networks of which the user is a member, including the groups' Meta Platforms group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Meta Platforms applications.

25. Meta Platforms also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Meta Platforms, including information about the type of action, the date and time of the

action, and the user ID and IP address associated with the action. For example, if a user views a Meta Platforms profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from which IP address the user did so.

26. Social networking providers like Meta Platforms typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Meta Platforms users may communicate directly with Meta Platforms about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta Platforms typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

27. In my training and experience, I have learned that social networking providers like Meta Platforms typically keep records that can reveal multiple Meta Platforms accounts accessed from the same electronic device, such as the same computer or mobile phone, including accounts that are linked by "cookies," which are small pieces of text sent to the user's Internet browser when visiting websites. This warrant requires Meta Platforms to identify any other accounts accessed by the same browser that accessed the SUBJECT ACCOUNT described in Attachment A, including accounts linked by cookies, recovery or secondary email address, or telephone number. This warrant asks that Meta Platforms identify such accounts and produce associated subscriber information.

28. According to Meta Platforms's current Data Policy, which is publicly available on the Internet, Meta Platforms also collects other device information, including information from or about the computers, phones, or other devices where the user installed or accessed Meta Platforms's Services, attributes such as the operating system, hardware version, device settings, file and software names and types, battery and signal strength, and device identifiers. Meta Platforms's Data Policy also states that it collects device locations, including specific geographic locations, such as through GPS, Bluetooth, or WiFi signals, as well as connection information such as the name of the user's mobile operator or ISP, browser type, language and time zone, mobile phone number and IP address.

29. Furthermore, Meta Platforms's Data Policy indicates that it collects information from websites and apps that use Meta Platforms's Services, such as information collected by Meta Platforms when the user of an account visits or uses third-party websites and apps that use Meta Platforms's Services, including information about the websites and apps the user visited, the user's use of Meta Platforms's Services on those websites and apps, as well as information the developer or publisher of the app or website provides to the user or to Meta Platforms.

30. As explained herein, information stored in connection with a Meta Platforms account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Meta Platforms user's "Neoprint," IP log, stored electronic communications, and other data retained by Meta Platforms, can indicate who has used or controlled the Meta Platforms account. This "user attribution" evidence is analogous to the search for "indicia of

occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Meta Platforms account at a relevant time. Further, Meta Platforms account activity can show how and when the account was accessed or used. For example, as described herein, Meta Platforms logs the IP addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Meta Platforms access, use, and events relating to the crime under investigation. Additionally, Meta Platforms builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Meta Platforms "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Meta Platforms account owner. Last, Meta Platforms account activity may provide relevant insight into the Meta Platforms account owner's state of mind as it relates to the offense under investigation. For example, information on the Meta Platforms account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

31. Therefore, the computers of Meta Platforms are likely to contain all the material described above, including stored electronic communications and information concerning

subscribers and their use of Meta Platforms, such as account access information, transaction information, and other account information.

JURISDICTION AND AUTHORITY TO ISSUE THE WARRANT

32. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

33. A search warrant under § 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

34. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

PROBABLE CAUSE

35. Deputies of the USMS began an investigation in attempt to locate and arrest Callahan on the outstanding escape. Throughout the investigation, USMS deputies learned Callahan is utilizing and signing into Meta Platforms using the vanity name "Hoss Boss".

36. On May 2, 2023, an open-source search of Facebook page https://www.facebook.com/profile.php?id=100087761752755 bears the vanity name "Hoss Boss". The profile photograph displays Callahan wearing a light blue shirt with two gold chains. A photograph posted on April 28, 2023, at 7:11pm indicates "Winners find a way. Losers find an excuse". Callahan appears to consistently post on the account as far back as February 23rd, 2023.

37. Callahan likely has knowledge investigators are actively searching for his whereabouts. As part of the USMS efforts to locate and eventually arrest Callahan, investigators need to obtain pertinent information regarding Callahan 's whereabouts, and associates who may be aiding him. Fugitives often use social media as a means of communication with associates through Messenger, direct messages and commenting on other profile pages. Fugitives frequently document their whereabouts on "reels" which may only be viewed for a limited time. Obtaining social media information from Callahan's account will allow investigators to gain further intelligence regarding Callahan's criminal activity, social circle, identify whom he may be residing with, and ultimately pinpoint his whereabouts.

38. Based upon this investigator's investigative experience, the applicant believes that from the Information gained from the SUBJECT ACCOUNT, a past and current location can be developed for Callahan.

REVIEW OF THE INFORMATION OBTAINED PURSUANT TO THE WARRANT

39. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Meta to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B.

Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

40. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to the Provider, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel within 30 days from the date of service. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the electronically-stored information and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the violation of 18 U.S.C. § 751(a) as specified in Attachment B to the proposed warrant.

41. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the 18 U.S.C. § 751(a), including but not limited to undertaking a cursory inspection of all messages within the SUBJECT ACCOUNT. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails or other electronic communications, including attachments such as scanned

documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords for which an agent is likely to search.

CONCLUSION

42. Based on the foregoing, I submit that there is probable cause to search the SUBJECT ACCOUNT described in Attachment A for the items described in Attachment B, and I therefore respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.

Respectfully submitted,

Danielle Shimchick
Deputy U.S. Marshal
U.S. Marshal Service

Subscribed and sworn to before me on May 4, 2023.

/s/ MRC
Mark R. Colombell
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF META PLATFORMS, INC. PROFILE ID ://www.facebook.com/profile.php?id=100087761752755	Case No. 3:23sw71 **FILED UNDER SEAL**

ATTACHMENT A

Property to be searched

This warrant applies to information associated with the **Meta Platforms User ID:** https://www.facebook.com/profile.php?id=100087761752755 (the "SUBJECT ACCOUNT") that is stored at premises owned, maintained, controlled, or operated by Meta Platforms Inc., a company headquartered in Menlo Park, California.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF META PLATFORMS, INC. PROFILE ID ://www.facebook.com/profile.php?id=100087761752755	Case No. 3:23sw71 **FILED UNDER SEAL**

ATTACHMENT B

Particular things to be seized

I. Information to be disclosed by Meta Platforms

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta Platforms, Inc. ("Meta Platforms"), including any messages, records, files, logs, or information that have been deleted but are still available to Meta Platforms, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta Platforms is required to disclose the following information to the government for the SUBJECT ACCOUNT listed in Attachment A from each account's creation to the present:

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Meta Platforms passwords, Meta Platforms security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;

(b) All address books uploaded, synched, or imported with/to the account;

(c) All records of Meta Platforms searches performed by the account;

(d) All deleted content associated with the account if still available or stored by Meta Platforms;

(e) All activity logs for the account and all other documents showing the user's posts and other Meta Platforms activities, such as content viewed or engaged with;

(f) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;

(g) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Meta Platforms user identification numbers; groups and networks of which the user is a member, including the groups' Meta Platforms group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Meta Platforms applications;

(h) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, deleted messages if still retained by Meta Platforms, and pending "Friend" requests;

(i) All "check ins" and other location information;

(j) All IP logs, including all records of the IP addresses that logged into the account;

(k) All records of the account's usage of the "Like" feature, including all Meta Platforms posts and all non-Meta Platforms webpages and content that the user has "liked";

(l) All information about the Meta Platforms pages that the account is or was a "fan" of;

(m) All past and present lists of friends created by the account;

(n) All login and logout records relating to the account;

(o) All information about the user's access and use of Meta Platforms Marketplace;

(p) The types of service utilized by the user;

(q) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(r) All privacy settings and other account settings, including privacy settings for individual Meta Platforms posts and activities, and all records showing which Meta Platforms users have been blocked by the account;

(s) All records pertaining to communications between Meta Platforms and any person regarding the user or the user's Meta Platforms account, including contacts with support services and records of actions taken;

(t) Device information, including information from or about the computers, phones, or other devices where the user installed or accessed Meta Platforms's Services, attributes such as the operating system, hardware version, device settings, file and software names and types, battery and signal strength, and device identifiers;

(u) Device locations, including specific geographic locations, such as through GPS, Bluetooth, or WiFi signals;

(v) Connection information such as the name of the user's mobile operator or ISP, browser type, language and time zone, mobile phone number and IP address;

(w) Information from websites and apps that use Meta Platforms's Services, such as information collected by Meta Platforms when the user of the account listed in Attachment A visited or used third-party websites and apps that use Meta Platforms's Services, including information about the websites and apps the user visited, the user's use of Meta Platforms's Services on those websites and apps, as well as information the

developer or publisher of the app or website provides to the user or to Meta Platforms; and

(x) For all Meta Platforms accounts that are linked to or associated with the SUBJECT ACCOUNT listed in Attachment A by machine cookies, secondary or recovery email address or telephone number, provide:

- Names (including subscriber names, user names, and screen names);
- Addresses (including mailing addresses, residential addresses, business addresses, and email addresses);
- Local and long distance telephone connection records;
- Records of session times and durations and IP address history logs;
- Records of login and logout history logs;
- Length of service (including start date) and types of service utilized;
- Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), MSISDN, International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Station Equipment Identities ("IMEI"));
- Other subscriber numbers or identities (including temporarily assigned network addresses and registration IP addresses (including carrier grade natting addresses or ports)); and

- Means and source of payment for such service (including any credit card or bank account number) and billing records.

II. Information to be seized by the government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and outside technical experts under government control) are authorized to review the records produced by Meta Platforms. They may conduct this review in order to: (a) locate Callahan, a person to be arrested pursuant to a federal arrest warrant issued by this district including, the fruits, evidence, and instrumentalities of a violation of 18 U.S.C. § 751(a), for the account listed on Attachment A, including information pertaining to the following matters:

(a) Any information relating to Callahan's location, including communications about visiting others;

(b) evidence that can help establish the identity of the SUBJECT ACCOUNT'S user(s), as well as the identities of any individuals providing residence and or aid to Callahan

(c) information related to the geographic location of the SUBJECT ACCOUNT'S user(s) and the geographic location of any co-conspirators

(d) passwords or other information needed to access user's computer or other online accounts.